**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A layer 2 network access device for providing network security, comprising: a plurality of input ports;

   a switching fabric in the layer 2 network access device for routing data received on said plurality of input ports to at least one output port; and

   control logic in the layer 2 network access device adapted to authenticate a physical address of a user device coupled to one of said plurality of input ports, to authenticate user information provided by a user of said user device only if said physical address is valid, and to restrict access to said one of said plurality of input ports in accordance with a user policy associated with said user information only if said user information is valid.

2. (Original) The network access device of claim 1, wherein said physical address comprises a Media Access Control (MAC) address.

3. (Original) The network access device of claim 1, wherein said control logic is adapted to authenticate said user information in accordance with an IEEE 802.1x protocol.

4. (Original) The network access device of claim 1, wherein said user policy identifies an access control list.

5. (Original) The network access device of claim 1, wherein said user policy includes an access control list.

6. (Original) The network access device of claim 1, wherein said user policy identifies a Media Access Control (MAC) address filter.

7. (Original) The network access device of claim 1, wherein said user policy includes a Media Access Control (MAC) address filter.

8. (Original) The network access device of claim 1, wherein said control logic is adapted to send said user information to an authentication server and to receive an accept message from said authentication server if said user information is valid.

9. (Original) The network access device of claim 8, wherein said authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

10. (Original) The network access device of claim 8, wherein said accept message includes said user policy.

11. (Original) The network access device of claim 1, wherein said control logic is further adapted to assign said one of said plurality of input ports to a virtual local area network (ULAN) associated with said user information if said user information is valid.

12. (Original) The network access device of claim 11, wherein said control logic is adapted to receive a message from an authentication server, wherein said message comprises a VLAN

identifier (ID) associated with said user information, and to assign said one of said plurality of input ports to a ULAN associated with said VLAN ID.

13. (Currently Amended) A method for providing network security, comprising:

authenticating in a layer 2 network access device a physical address of a user device coupled to a port of ~~a~~ the network access device;

authenticating user information provided by a user of said user device to the network access device only if said physical address is valid; and

restricting access to said port in accordance with a user policy associated with said user information only if said user information is valid.

14. (Original) The method of claim 13, wherein said authenticating a physical address comprises authenticating a Media Access Control (MAC) address.

15. (Original) The method of claim 13, wherein said authenticating said user information comprises authenticating said user information in accordance with an IEEE 802.1x protocol.

16. (Original) The method of claim 13, wherein said restricting access comprises restricting access to said one of said plurality of input ports in accordance with an access control list.

17. (Original) The method of claim 13, wherein said restricting access comprises restricting access to said one of said plurality of input ports in accordance with a Media Access Control (MAC) address filter.

18. (Original) The method of claim 13, wherein said authenticating said user information comprises:

sending said user information to an authentication server; and receiving an accept message from said authentication server if said user information is valid.

19. (Original) The method of claim 18, wherein said authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

20. (Original) The method of claim 18, wherein said receiving an accept message comprises receiving an accept message that includes said user policy.

21. (Original) The method of claim 13, further comprising:

assigning said port to a virtual local area network (VLAN) associated with said user information only if said user information is valid.

22. (Original) The method of claim 21, wherein said assigning said port to a VLAN comprises:

receiving a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information; and

assigning said port to a VLAN associated with said VLAN ID.

23. (Currently Amended) A network system, comprising: a data communications network;

a layer 2 network access device coupled to said data communications network;

and

a user device coupled to a port of said network access device;

wherein said network access device is adapted to authenticate a physical address of said user device, to authenticate user information provided by a user of said user device only if said physical address is valid, and to restrict access to said port in accordance with a user policy associated with said user information only if said user information is valid.

24. (Original) The system of claim 23, wherein said physical address comprises a Media Access Control (MAC) address.

25. (Original) The system of claim 23, wherein said network access device is adapted to authenticate said user information in accordance with an IEEE 802. lx protocol.

26. (Original) The system of claim 23, wherein said user policy identifies an access control list.

27. (Original) The system of claim 23, wherein said user policy includes an access control list.

28. (Original) The system of claim 23, wherein said user policy identifies a Media Access Control (MAC) address filter.

29. (Original) The system of claim 23, wherein said user policy includes a Media Access Control (MAC) address filter.

30. (Original) The system of claim 23, further comprising:

an authentication server coupled to said data communications network;

wherein said network access device is adapted to send said user information to said authentication server and to receive an accept message from said authentication server if said user information is valid.

31. (Original) The system of claim 30, wherein said authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

32. (Original) The system of claim 30, wherein said accept message includes said user policy.

33. (Original) The system of claim 23, wherein said network access device is further adapted to assign said port to a virtual local area network (VLAN) associated with said user information if said user information is valid.

34. (Original) The system of claim 33, further comprising:

an authentication server coupled to said data communications network;

wherein said network access device is adapted to receive a message from said authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information, and to assign said port to a VLAN associated with said VLAN ID if said user information is valid.

35. (New) The network access device of claim 2 wherein said control logic is further configured to:

if authentication of said MAC address indicates said MAC address is invalid,

drop packets from said user device; or

disable said port;

if authentication of said user information indicates said user information is invalid, block all traffic on said port except for packets related to a user authentication protocol;

if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said network access device;

if said user is not associated with said VLAN,

assign said port to a port default VLAN; and

block all traffic on said port except for packets related to said user authentication protocol; and

if said user is associated with said VLAN,

assign said port to said VLAN associated with said user; and

forward packets from said user device.

36. (New) The method of claim 14, further comprising:

if said authenticating of said MAC address indicates said MAC address is invalid,

dropping packets from said user device; or

disabling said port;

if said authenticating user information indicates said user information is invalid, blocking all traffic on said port except for packets related to a user authentication protocol;

if said authenticating user information indicates said user information is valid, determining whether said user is associated with a VLAN supported by said network access device;

if said determining indicates said user is not associated with said VLAN,

assigning said port to a port default VLAN; and

blocking all traffic on said port except for packets related to said user authentication protocol; and

if said determining indicates said user is associated with said VLAN,

assigning said port to said VLAN associated with said user; and

forwarding packets from said user device.

37. (New) The network system of claim 24 wherein said network access device is further adapted to:

if authentication of said MAC address indicates said MAC address is invalid,

dropping packets from said user device; or

disabling said port;

if authentication of said user information indicates said user information is invalid, block all traffic on said port except for packets related to a user authentication protocol;

if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said network access device;

if said user is not associated with said VLAN,

assign said port to a port default VLAN; and

block all traffic on said port except for packets related to said user authentication protocol; and

if said user is associated with said VLAN,

assign said port to said VLAN associated with said user; and

forward packets from said user device.

38. (New) An apparatus for providing network security, comprising:

a plurality of input ports;

a switching fabric for routing data received on said plurality of input ports to at least one output port; and

control logic adapted to:

authenticate a physical address of a user device coupled to one of said plurality of input ports;

drop packets from said user device if said physical address is invalid;

authenticate user information provided by a user of said user device only if said physical address is valid;

if authentication of said user information indicates said user information is invalid, block all traffic on said one of said plurality of input ports except for packets related to a user authentication protocol;

if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said apparatus by receiving a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information;

if said user is not associated with said VLAN,

assign said one of said plurality of input ports to a port default VLAN; and

block all traffic on said one of said plurality of input ports except for packets related to said user authentication protocol; and

if said user is associated with said VLAN,

assign said one of said plurality of ports to said VLAN associated with said user; and

restrict access to said one of said plurality of input ports in accordance with a user policy associated with said user information.

39. (New) The apparatus of claim 38, wherein said apparatus comprises a layer 2 network access device.

40. (New) A method for providing network security, comprising:

authenticating a physical address of a user device coupled to a port of a network access device;

dropping packets from said user device if said physical address is invalid;

authenticating user information provided by a user of said user device only if said physical address is valid;

if said authenticating of said user information indicates said user information is invalid, blocking all traffic on said port except for packets related to a user authentication protocol;

if said authenticating of said user information indicates said user information is valid, determining whether said user is associated with a VLAN supported by said network access device by receiving a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information;

if said user is not associated with said VLAN,

assigning said one of said plurality of input ports to a port default VLAN; and

blocking all traffic on said one of said plurality of input ports except for packets related to said user authentication protocol; and

if said user is associated with said VLAN,

assigning said one of said plurality of ports to said VLAN associated with said user; and

restricting access to said one of said plurality of input ports in accordance with a user policy associated with said user information.

41. (New) The method of claim 40, wherein said network switch comprises a layer 2 network access device.

42. (New) A network system, comprising:

a data communications network;

a network access device coupled to said data communications network; and

a user device coupled to a port of said network switch, wherein said network access device is adapted to:

authenticate a physical address of a user device coupled to one of said plurality of input ports;

drop packets from said user device if said physical address is invalid;

authenticate user information provided by a user of said device only if said physical address is valid;

if authentication of said user information indicates said user information is invalid, block all traffic on said one of said plurality of input ports except for packets related to a user authentication protocol;

if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said network access

device by receiving a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information;

if said user is not associated with said VLAN,

assign said one of said plurality of input ports to a port default VLAN; and

block all traffic on said one of said plurality of input ports except for packets related to said user authentication protocol; and

if said user is associated with said VLAN,

assign said one of said plurality of ports to said VLAN associated with said user; and

restrict access to said one of said plurality of input ports in accordance with a user policy associated with said user information.

43. (New) The network system of claim 42, wherein said network access device comprises a layer 2 network access device.